整理番号:19948　　発送番号:313610　発送日:平成15年 9月 9日

拒絶理由通知書

15.9.27
I. P.

15.11.-7

特許出願の番号	平成１１年　特許願　第０１６２５７号
起案日	平成１５年　９月　１日
特許庁審査官	青木　重徳　　４２２９　５Ｍ００
特許出願人代理人	河野　登夫　様
適用条文	第２９条柱書、第２９条第２項、第３６条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

【Ａ】この出願の下記の請求項に記載されたものは、下記の点で特許法第２９条第１項柱書に規定する要件を満たしていないから、特許を受けることができない。

記

・請　求　項：１
・備　　考

計算法、作図法と認められる発明は、一般に人間の推理力や記憶力を利用するものであって自然法則利用の技術的手段を伴うものでないから、特許法第２条に定義されている発明とは認められず、同法第２９条の特許要件を備えていないと解するのが原則である。

そして、請求項１はセンタとエンティティ間で分割特定情報を利用して秘密鍵を生成する計算手続きを記載したものであり、自然法則利用の技術的手段を伴うものでないから、上記原則が適用できる。

・請　求　項：２
・備　　考

文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。

そして、請求項２は分割特定情報を利用して生成した秘密鍵に基づいて共通鍵を生成し、該共通鍵により平文を暗号文に暗号化する方法について記載したもの

であり、その間何らの装置を用いず、自然法則利用の技術的手段を施していないことから、上記原則が適用できる。

・請　求　項：３－６
・備　　考
文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、これを暗号による通信方法と解しても暗号による思想表現の方法と認められ、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。
そして、請求項３－６には分割特定情報を利用して生成した秘密鍵に基づいて共通鍵を生成し、該共通鍵を用いて暗号通信を行う方法が記載されており、その間何らの装置を用いず、自然法則利用の技術的手段を施していないことから、上記原則が適用できる。

・請　求　項：７
・備　　考
文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、これを暗号による通信方法と解しても暗号による思想表現の方法と認められ、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。
しかしながら、請求項7に係る発明は「暗号通信システム」について記載した物の発明であることから、上記原則にはあたらないとも考えられるが、請求項７に実質的に記載されている内容は、分割特定情報を利用して生成した秘密鍵に基づいて共通鍵を生成し、該共通鍵を用いて暗号通信を行う方法であり、その間何らの装置を用いず、自然法則利用の技術的手段を施していないことから、上記原則を類推適用できる。

請求項１－７に記載されたものは特許法第２９条第１項柱書でいう発明に該当しないことが明らかであるから、当該請求項に記載のものについては新規性、進歩性等の特許要件についての審査を行っていない。

【Ｂ】この出願の下記の請求項に係る発明は、その出願前日本国内において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　（引用文献等については引用文献等一覧参照）

・請　求　項：８

・引用文献等：１，２

・備　　考

引用文献１には、「６　むすび」において、「センタが必ずしも信頼できるとは限らない。もし、センタが不正を行えば全てのエンティティ間の鍵を生成することができる。このようにセンタの権限が大きすぎるという問題がある。」点に着目して、複数の信頼のおけるセンタの存在を仮定し、エンティティはそれぞれのセンタの秘密鍵に基づいて共有鍵を生成し、さらに、日時などの変動パラメータを用いて加工することで、実際の通信に用いる最終共通鍵を求めるなどの対策が必要となる旨が示唆されており、またＩＤ情報に基づく予備通信不要な鍵共有方式として、センタはエンティティのＩＤからｎ次元の公開鍵ベクトルを計算し、該公開鍵を用いて計算した秘密鍵を秘密裏に送っておき、通信を希望するエンティティ間で鍵共有を行う共通鍵生成装置が記載されている。

引用文献２には、単一の鍵発行センタが端末の秘密鍵を生成するため、その鍵発行センタは端末の秘密鍵を容易に知ることができ、鍵発行センタによって端末の秘密鍵を悪用されかねたいという問題点に着目し、鍵発行センタを複数の鍵生成サブセンタにて構成し、秘密鍵生成依頼を行う際に端末分割部にて端末秘密情報を分割して各鍵生成サブセンタに配送し端末秘密鍵情報の要求を行い、各鍵生成サブセンタは端末識別情報をディジタル署名部にて入力して端末部分秘密鍵を生成し、端末側では受信した端末部分秘密鍵と前記端末秘密情報から端末秘密鍵情報を生成する鍵生成技術が記載されている。

そして、引用文献１，２が共にセンタの不正を技術課題とした鍵生成技術について記載したものである点を勘案すれば、引用文献１に記載されている共通鍵生成装置において、引用文献２に記載されている鍵生成技術を採用し、複数の信頼のおけるセンタに対してエンティティのＩＤを分割したものを送り、それに応じて各センタから送られてきた部分秘密鍵を統合して得た秘密鍵に基づいて通信を希望するエンティティ間で共通鍵を生成できるよう構成することは、当業者が容易になし得ることである。

・請　求　項：９

・引用文献等：１，２

・備　　考

引用文献１には、「６　むすび」において、「センタが必ずしも信頼できるとは限らない。もし、センタが不正を行えば全てのエンティティ間の鍵を生成することができる。このようにセンタの権限が大きすぎるという問題がある。」点に着目して、複数の信頼のおけるセンタの存在を仮定し、エンティティはそれぞれのセンタの秘密鍵に基づいて共有鍵を生成し、さらに、日時などの変動パラメー

タを用いて加工することで、実際の通信に用いる最終共通鍵を求めるなどの対策が必要となる旨が示唆されており、またＩＤ情報に基づく予備通信不要な鍵共有方式として、センタはエンティティのＩＤからｎ次元の公開鍵ベクトルを計算し、該公開鍵を用いて計算した秘密鍵を秘密裏に送っておき、通信を希望するエンティティ間で鍵共有を行う共通鍵生成方法が記載されている。

引用文献２には、単一の鍵発行センタが端末の秘密鍵を生成するため、その鍵発行センタは端末の秘密鍵を容易に知ることができ、鍵発行センタによって端末の秘密鍵を悪用されかねたいという問題点に着目し、鍵発行センタを複数の鍵生成サブセンタにて構成し、秘密鍵生成依頼を行う際に端末分割部にて端末秘密情報を分割して各鍵生成サブセンタに配送し端末秘密鍵情報の要求を行い、各鍵生成サブセンタは端末識別情報をディジタル署名部にて入力して端末部分秘密鍵を生成し、端末側では受信した端末部分秘密鍵と前記端末秘密情報から端末秘密鍵情報を生成する鍵生成技術が記載されている。

そして、引用文献１，２が共にセンタの不正を技術課題とした鍵生成技術について記載したものである点を勘案すれば、引用文献１に記載されている共通鍵生成方法において、引用文献２に記載されている鍵生成技術を採用し、複数の信頼のおけるセンタに対してエンティティのＩＤを分割したものを送り、それに応じて各センタから送られてきた部分秘密鍵を統合して得た秘密鍵に基づいて通信を希望するエンティティ間で共通鍵を生成できる方法とすることは、当業者が容易になし得ることであるし、このような方法をコンピュータネットワーク上で実現するために、プログラムコード化して記録媒体に記録しておくことは、当業者にとって常套手段である。

引　用　文　献　等　一　覧

１．藤川篤則，村上恭通，笠原正雄，“計算量的に安全なＩＤ－ＮＩＫＳ”，
電子情報通信学会技術研究報告（ＩＳＥＣ９６－１９），日本，
社団法人電子情報通信学会，１９９６年　７月２２日，
Ｖｏｌ．９６，Ｎｏ．１６７，ｐ．１２７－１３２
２．特開平４－２４５２８７号公報

【Ｃ】この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。

記

本願請求項８，９には「エンティティ」という要素が発明として用いられているが、該「エンティティ」が何を示すのか、択一的に記載されていないことから発明が不明瞭である。

つまり、一般に「エンティティ」とは通信を担う人物や、人物が操作する装置を意味しており、本願明細書の記載内容からだけでは請求項に記載されている「

エンティティ」がそのいずれなのかが明確に区別できない。

よって、請求項８，９に係る発明は明確でない。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

先行技術文献調査結果の記録

・調査した分野　ＩＰＣ第７版

Ｈ０４Ｌ９／０８

・先行技術文献

辻井重男，村上恭通，笠原正雄：“第四の鍵共有方式－拡張ＩＤ－ＮＩＫＳの提案”，１９９９年暗号と情報セキュリティシンポジウム予稿集，１９９９．０１．２６，Ｖｏ．１／２，ｐ．１３５－１４０

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。